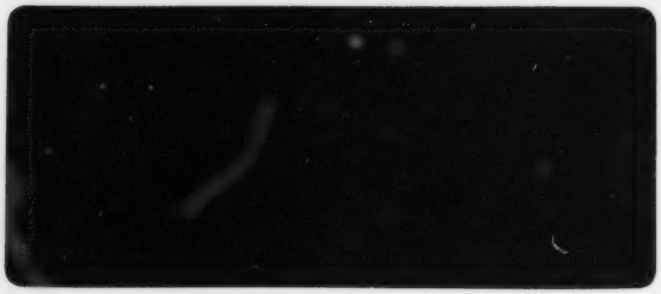
ACNS
CCSN

Advisory Committee on Nuclear Safety
Comité consultatif de la sûreté nucléaire

Advisory Committees of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9
Comités consultatifs de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9



COMMITTEE REPORTS

Since the 1950's the Atomic Energy Control Board has made use of advisory committees of independent experts to assist it in its decision-making process. In 1979 the Board restructured the organization of these consultative groups, resulting in the creation of two senior level scientific committees charged with providing the Board with independent advice on principles, standards and general practices related to radiation protection and the safety of nuclear facilities. The two committees are the Advisory Committee on Radiological Protection (ACRP), formed in 1979, and the Advisory Committee on Nuclear Safety (ACNS), which was established a year later. Summaries of meetings of the committees are available to the public in the AECB library in Ottawa.

From time to time the committees issue reports which are normally published by the AECB and catalogued within the AECB's public document system. Committee reports, bound with a distinctive cover, carry both a committee-designated reference number, e.g. ACRP-1, and an AECB reference number in the "INFO" series. The reports generally fall into two broad categories: (i) recommendations to the Board on a particular technical topic, and (ii) background studies. **Unless specifically stated otherwise, publication by the AECB of a committee report does not imply endorsement by the Board of the content, nor acceptance of any recommendations made therein.**

RAPPORTS DES COMITÉS

Depuis les années cinquante, la Commission de contrôle de l'energie atomique fait appel à des comités consultatifs composés d'experts indépendants pour l'aider dans ses prises de décision. En 1979, la CCEA a restructuré l'organisation de ces groupes de consultation pour former deux comités scientifiques supérieurs chargés de lui fournir des conseils indépendants concernant les principes, les normes et les méthodes générales touchant la radioprotection et la sûreté des installations nucléaires : ce sont le Comité consultatif de la radioprotection (CCRP), formé en 1979, et le Comité consultatif de la sûreté nucléaire (CCSN), établi l'année suivante. Le public peut consulter les comptes rendus des réunions de ces comités à la bibliothèque de la CCEA, à Ottawa.

Les comités rédigent à l'occasion des rapports qui sont normalement publiés par la CCEA et catalogués dans la collection des documents publics de la CCEA. Reliés avec une couverture distincte, les rapports des comités se reconnaissent à leur numéro de référence du comité d'origine (comme CCRP-1) et à leur numéro de référence de la CCEA dans la série «INFO». Ils se divisent habituellement en deux catégories générales : (i) les recommandations présentées à la Commission au sujet d'une question technique particulière; (ii) les études générales. **À moins d'indication contraire, la publication par la CCEA du rapport d'un comité ne signifie pas que la Commission approuve le contenu de la publication, ni qu'elle en accepte les recommandations.**

Advisory Committees of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comités consultatifs de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

92-04619/

INFO-0359 (E)

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

ACNS-17

Improving the Safety Culture of Human Organizations: A Proposal For Institutional Quality Assurance

by the

Advisory Committee on
Nuclear Safety

February 1990

An Advisory Committee of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

ABSTRACT

Inquiries into past serious accidents, both nuclear and non-nuclear, reveal that the causes, largely attributed to human error, are also failures on the part of the institutions responsible. Conventional wisdom holds that quality assurance is an essential element for any production process, but the inquiries have not suggested applying quality assurance to the institutions themselves. The ACNS argues the need for Institutional Quality Assurance, with some illustrations of what might be involved, and proposes what should be done to achieve this end.

Table of Contents

	Page
ABSTRACT	(i)
Table of Contents	(ii)
1. INTRODUCTION	1
2. INSTITUTIONAL FAILURES	2
2.1 Approach	2
2.2 Serious Reactor Accidents	3
2.2.1 Windscale (U.K.)	3
2.2.2 Three Mile Island (U.S.A.)	4
2.2.3 Chernobyl (U.S.S.R.)	4
2.3 CANDU Experience	5
2.4 Conclusion	6
3. A ROLE FOR QA	6
4. PROPOSED MEASURES	9
References	11
APPENDICES	
Appendix 1	1-1
Appendix 2	2-1
Appendix 3	3-1
Acknowledgements	

1. INTRODUCTION

Those concerned with nuclear safety are becoming increasingly aware of the importance of *"safety culture"* in institutions with nuclear-related activities. There is still disagreement over the precise meaning of the term, but most people know of institutions whose members have a better attitude to safety than others.

F.K. Hare, Commissioner of the Ontario Nuclear Safety Review (ONSR), devoted a section of the Review's report to "Ontario Hydro's Safety Culture" [1]. In it he said:

> *"There can be no doubt about Ontario Hydro's dedication to maintaining safety. What is not discussed in any depth [in their submission] is the corporation's safety culture, the expression used by industrial engineers to comprehend the entire atmosphere surrounding the maintenance of safety, informal as well as formal. To use another cant phrase of the day, the hidden safety agenda also affects the outcome, perhaps decisively."*

And later he posed the questions:

> *"How does a large institution ensure that its present high standards endure or improve? How can Ontario Hydro achieve this? These are not rhetorical questions. Other public utilities have seen their competence wither away, just as private corporations have degenerated without any good reason. .... Could this happen to Ontario Hydro?"*

The Atomic Energy Control Board's Advisory Committee on Nuclear Safety (ACNS), in its report ACNS-15 [2] commenting on the ONSR Report, made several relevant recommendations. In particular, one (No. 6) stated:

> *"The ACNS recommends that the AECB support studies into the factors of a sound 'safety culture', so as to be able to identify any weakness in this area in organizations."*

In selecting an approach to ensure a sound safety culture, the ACNS took notice of another quotation from the ONSR Report [1]:

> *"In a review of these submissions [to the ONSR], J.A.L. Robertson (writing personally as a consultant)* argued strongly that the maintenance of quality in the performance of institutions was as important as material QA for safety."*

Accordingly, the ACNS initiated a study with the following terms of reference:

- To examine whether institutional failings, as distinct from component failures and human errors, have contributed significantly to past reactor accidents and unforeseen occurrences (Significant Events in Ontario Hydro parlance)

---

* Since appointed a member of the ACNS.

- to consider whether the principles and methods of Quality Assurance (QA) can be applied or adapted to reduce the likelihood of future institutional failings, and

- if appropriate, to recommend what initiatives should be taken, and by whom, to implement Institutional Quality Assurance (IQA) for nuclear energy.

Each of these three terms of reference is addressed in turn in the following sections of this report.

2. INSTITUTIONAL FAILINGS

2.1 Approach

Accidents are the most obvious indications of deficiencies in safety. Generally, accident investigations have assigned responsibility for the accident to one or more of three broad causes: design error, component failure and human error.

However, it has become apparent that *"human error"* does not always describe adequately errors in which some person was the instrument. All too often, the underlying cause of the accident was a failure on the part of the institution to which the person belonged to have instituted or ensured proper safety precautions. These are institutional failings.

Mosey and Weaver identified this cause of accidents in a presentation to the 1988 Annual Meeting of the Canadian Nuclear Society [3]. In their paper, "A Discussion of Institutional Failure and its Importance to Nuclear Safety", they surveyed and analyzed the causes of eight accidents. They concluded that:

> *"Institutional failure can be identified in a significant fraction of these accidents .... [where] the term means that some function which is necessary or desirable for safety is either absent or not functioning to some minimum criterion."*

The authors emphasized the need to develop a better definition of institutional failure.

The ACNS has adopted the following:

> **In the context of nuclear safety, an institutional failing is a breach of safety in which the cause extends within the relevant institution beyond the immediate agent, whether a failed component or a person who erred.**

Institutional failings are not confined to the nuclear industry -- far from it. For instance, following an aircraft crash in the US it was said that flight crews do not always perform pre-takeoff checks and may switch off certain instruments. After the shooting down of Iran Air Flight #655 it was said that Iran Air pilots regularly disregarded demands by the US Navy to identify themselves. The UK's inquiry into a disastrous fire at King's Cross Underground Station assigned responsibility to the top management of London Transport for having failed to ensure the existence of adequate protective measures even after

previous fires of a similar nature. Following the Alaskan oil spill from the Exxon Valdez, it was reported that the supertanker's captain, with an alleged alcohol problem, was checked after the accident and was found to have a blood-alcohol content above the legal limit; and that the third mate was officer of the watch although he was not licensed for these waters. In Canada, an inquiry into the collapse of a supermarket on its opening day found that the roof had not been built properly and identified institutional failings on the part of the project's engineering firm and of the regulatory body.

What is most worrying is that in all these instances the violations were said to be general knowledge, but the institutions concerned had taken little or no action. It is not surprising, therefore, that the public has become disillusioned over claimed safety precautions for many technologies. Increasingly heard are *"The system failed us", "They said this could not happen"* and *"Why should we trust you now?"*.

The ACNS recognizes that these unsubstantiated media reports do not constitute proof that institutional failings are a widespread problem. They do, however, suggest that institutional failings may be a cause of deficiencies in safety that has not received sufficient attention. The ACNS therefore examined whether there are authenticated instances of institutional failings in nuclear institutions. The approach adopted was to review inquiries into past nuclear accidents, since these provide the most thoroughly investigated and documented studies into the causes of breaches in safety. The three accidents reviewed were selected for a combination of criteria:

- relevance to power reactors, e.g., relatively high power
- relevance to public safety, e.g., actual or potential release of radioactive materials
- relevant documentation available
- relevance of results to the public, e.g., public awareness of the accident.

Since none of these three accidents occurred in Canada, the ACNS also examined what could be learned about institutional failings from a review of reports of the most serious incidents to have occurred in CANDU reactors.

2.2 Serious Reactor Accidents

2.2.1 Windscale (U.K.)

On the 10th of October, 1957, the metallic uranium fuel and the graphite moderator of one of the plutonium-production reactors at Windscale, U.K., caught fire as a result of scheduled low-power operation during a period of reactor maintenance. With virtually no reactor containment, as the term is now understood, large amounts of radioactive material were released and spread across the U.K. as well as several countries in Northern Europe. Although no immediate fatalities or injuries resulted, the releases may have caused some increase in the incidence of cancer in the areas affected.

A Committee of Inquiry into the accident reported its findings [4] later the same month. According to Mosey and Weaver [3]:

> *"The principal technical defect contributing to the accident, the Committee determined, was the inadequacy of instrumentation for the 'safe and proper operation' of a Wigner release. In addition, however, the Committee identified the almost complete lack of operating documentation as a 'serious defect' and pointed to a number of 'deficiencies and inadequacies' of organization including a lack of definition of division of responsibilities and 'undue reliance on technical direction by committee'. As well, it was noted that the operations staff at Windscale were 'not well supported in all respects by technical advice' .... ."*

2.2.2 Three Mile Island (U.S.A.)

On the 28th of March, 1979, Unit 2 (a pressurized water reactor) of the nuclear generating station at Three Mile Island, Pennsylvania, U.S.A., suffered a loss-of-coolant accident that led to partial melting of the core. Despite the severity of the physical damage to the reactor the vast majority of the radioactive inventory was retained within the containment. The small amounts of radioactive materials that were released were estimated to have caused radiation doses to the most exposed members of the public of about the same amount as their annual doses from natural sources (i.e., background radiation).

The Report of the (U.S.) President's Commission on the Accident at Three Mile Island, chaired by John G. Kemeny [5], revealed some faults in design and components and some human errors at the operator level, but also identified many deficiencies in the institutions concerned. In the ACNS's view the major causes of the accident were to be found in the deficiencies in the utility and in the regulatory agency, i.e., institutional failings. Many of the report's recommendations addressed these deficiencies.

A summary of the causes of this accident is to be found in Appendix 1. When these were examined in detail, many were found not to be the fault of the individual operators, designers, etc., but of the institutions to which they belonged. Furthermore, the occurrence of so many coincidental faults argues strongly for failings on the part of the institutions concerned, the design organization, the operating utility and the regulatory agency. Under the heading "Institutional Failings" in this and the other appendices, the institutional failings which, in the judgement of the ACNS, contributed to the accident are identified.

2.2.3 Chernobyl (U.S.S.R.)

The world's worst reactor accident occurred at Chernobyl in the Ukraine, U.S.S.R., on the 26th of April, 1986. As a result of tests conducted by the operators on Unit 4 (a graphite-moderated, water-cooled reactor of the RBMK type) in the process of shutting down the reactor, a control instability developed: The power suddenly increased to about a hundred times the full-power value. This resulted in chemical explosions, ignition of the graphite, destruction of the reactor core and its building, and ejection of burning fragments over the surrounding area. The remaining graphite continued burning for more than ten days. This fire was a major contributory factor to the 31

deaths among station and emergency workers directly attributable to the effects of blast, radiation, and fire, and to the widespread dispersion of radioactive material over much of Europe, which may increase the risk of additional cancer deaths by some thousands over the next fifty years (but much less than one per cent of the cancer deaths expected from all other causes).

A subsequent meeting on the Chernobyl accident [7,8], held in Vienna and sponsored by the International Atomic Energy Agency (IAEA), revealed some fundamental weaknesses in the reactor design, but the overwhelming impression was of a combination of operator errors and misconduct that would have been incredible had it not actually happened. The USSR authorities attributed blame to the operators concerned and to the station management. However, those familiar with what happens in Canada cannot imagine how this chain of events could have occurred without gross failings on the part of the Soviet institutions concerned, the utility and the regulatory body. For reasons still not widely understood, these institutions failed to function in a manner that would prevent such gross violations. The IAEA, by not drawing attention to these institutional failings, has provided evidence of its own institutional failing. Until all these failings are identified and corrected there can be no justifiable confidence that such an accident will not recur. Justification for the conclusions in this paragraph is provided in Appendix 2.

2.3 CANDU Experience

The worst accident to a Canadian CANDU reactor occurred on the 1st of August, 1983. A pressure tube of Unit 2 of the Pickering-A Station ruptured while the reactor was at full power. The operators shut down the reactor using the normal process systems, i.e., without the need to invoke any of the safety systems. There were no injuries to station workers and no release of radioactive materials from the station, but the repairs were costly in economic terms.

Subsequent investigation [9,10] revealed that the fuel channel assemblies were not in the configuration intended in the design, because no provision had been made for positive location of spacer springs between the pressure and calandria tubes. These springs were not where they should have been, allowing contact between the two tubes. Thus the ostensible cause was essentially a design weakness compounded by inadequate conventional quality assurance (QA) during construction and commissioning.

What is most relevant in the present context is that all the information needed to prevent the pressure-tube rupture was available. The institutions concerned had failed to coordinate, appreciate and act on the information available. While these institutional failings caused no breach in occupational or public safety, their consequences were very costly.

Atomic Energy of Canada Limited (AECL) tabled at the ONSR a file [11] of the most serious incidents to have occurred in CANDU reactors, including the one just mentioned. Examination of this indicates that, while there is no evidence of institutional failings as serious as those that occurred at Windscale, Three Mile Island and Chernobyl, there is an obvious need for improved conventional QA. Appendix 3 provides details.

2.4 Conclusion

From consideration of these reactor accidents, as well as others not described here, the ACNS concludes that institutional failings have indeed contributed significantly to breaches of nuclear safety outside Canada. The ACNS also concludes that, while experience in Canada is generally satisfactory, some improvements in institutional performance are desirable.

3. A ROLE FOR QA

While the ACNS agrees with the ONSR Commissioner's conclusion [1] that:

> *"The Ontario Hydro reactors are being operated safely and at high standards of technical performance,"*

it also shares his concern that the present high standards might not be maintained in the future.

Once-proud institutions, such as the railways and postal service, have been seen to deteriorate over periods short compared with the expected life of a reactor system. The concern is not just for the normal ageing of institutions but for the organizational problems inherent in an institution that expands rapidly, or in one that has to contract. Also, public institutions are susceptible to political pressures which, while praiseworthy in their own rights, could conflict with the institutions' responsibilities for safety.

The ACNS therefore investigated what methods were available, or could be developed, to prevent institutional failings, thereby maintaining the present safety record of Canadian institutions and perhaps even improving the present situation. An additional benefit would be an increased public confidence in CANDU safety with an understanding of the safeguards against institutional failings.

Since quality assurance (QA) has proved itself very successful in reducing the incidence of faults in manufacturing, its application to the performance of institutions was examined.

The discipline of QA originated largely in the US military and aerospace programs, where the consequences of faults could be truly catastrophic. Now, however, there is widespread appreciation throughout industry of the economic benefits of QA. For example, the Ford Motor Company adopted the slogan: *"Quality is Job 1"*.

The definition of QA used here (but not universally assumed by those implementing QA programs) is:

> ***Quality Assurance*** **is the assemblage of all means required to assure with a high degree of confidence that the quality of all the components of an enterprise are appropriate to their purposes, so that the enterprise as a whole will perform as intended. The components include, but are not restricted to, materials, design, manufacture, construction, operational methods, human behaviour and performance of the institution as a whole. An essential element of quality assurance is an audit function, independent of the organizational structures directly responsible for the enterprise's individual components.**

An important part of the definition is that it does not necessarily require the highest quality for every constituent, but the quality appropriate to its purpose. In much the same way, a QA program should be appropriate. Insistence on an excessive and unjustified program for QA will inevitably be resisted.

In this report the safety benefits of QA are stressed. Others argue that the economic benefits are the principal motivation, so that QA ought to be embraced enthusiastically and not resisted as an extra cost, externally imposed. Both views are probably valid, with the balance between safety and economic benefits varying from industry to industry.

The Canadian nuclear industry accepts the need for, and value of, QA. The Canadian Standards Association has developed a series of standards entitled "Quality Assurance Program Requirements for Nuclear Power Plants" [12]. These cover many of the specific points raised in this report but, in practice, seem to be applied almost entirely at the working level. Also these standards do not apply to the regulatory agency, one of the institutions most important to nuclear safety and one which has provided instances of institutional failings in the foreign case studies examined by the ACNS (Section 2).

The AECB requires that an effective quality assurance program be established and implemented for each nuclear facility, and has defined proposed requirements for the program in its Consultative Document C-22 [13]. The ACNS, in its report ACNS-4, "Recommended General Safety Requirements for Nuclear Power Plants" [14], included requirements for appropriate QA in design and construction. Both the ONSR, in its report [1], and the IAEA, in its report "Basic Safety Principles for Nuclear Power Plants" [15], identified QA as one of the most important foundations on which nuclear safety is built. The ACNS, reviewing the IAEA document in its report ACNS-16 [16], noted that the IAEA had put more emphasis on safety culture than the ACNS had in its report ACNS-4, and endorsed this additional emphasis.

From this review of the existing literature it was evident that many of the constituent elements of a comprehensive QA program had already been identified within the Canadian nuclear industry and its regulatory agency. Although the principles and requirements applied to employees of the institutions concerned, there was an absence of any formal and integrated QA program for the institutions themselves. This omission was particularly notable in view of the fact that institutional failings were partly or largely responsible for the accidents at Three Mile Island and Chernobyl.

In examining how the methodology of QA might be applied to institutions, the ACNS first identified some of the discipline's more important principles. Expressed in terms applicable to institutions, these are (in alphabetic order):

Accountability. Institutions, as well as individuals, must be accountable for their actions.

Audit. The performance record of any institution having a potential effect on safety must be subject to audit.

Authorization. Institutions must ensure that no action may be taken without due authorization.

Independence. Auditing and regulation must be performed by individuals, groups or institutions organizationally independent of those responsible for implementing the activity concerned.

Integrity. Any information used by an institution and having a potential effect on safety must be of high integrity.

Measurement. Institutions' management systems must include processes to measure their performance.

Responsibility. Responsibilities, and demarcations between responsibilities, within the institution must be clearly assigned.

Traceability. All chains of responsibility and of reasoning within an institution must be clearly traceable.

Visibility. The total process must be as open as possible to public inspection.

Some possible ways in which these principles might be applied to institutions in a nuclear context include:

To the Regulatory Agency

1) The regulatory function must be independent of the other functions, e.g., design, research and development, promotion, marketing, and operation, to the greatest extent possible in the Canadian system of government.

2) The regulator must distinguish between policies, regulations, and guidelines, stating each explicitly and clearly.

3) The regulator must develop policies, regulations, and guidelines through a process that allows input from interested parties, e.g., the AECB's present use of consultative documents. Comments submitted, the disposition of them, and reasons for the disposition, must be documented.

4) The regulator must set requirements and goals in a form that can be monitored, preferably quantified: A requirement for which the compliance cannot be verified has little value.

5) The regulator must record and document its decisions, stating explicitly the reasons.

6) The regulator must audit the licensees' performance.

7) As much as possible of the documentation must be publicly accessible, including the comments on consultative documents and the summarized audits of licensees' performance.

To the Operating Utility

1) An institution applying for a licence must provide QA programs covering all aspects of the enterprise for regulatory approval: The regulator must audit these programs.

2) The design and all operating procedures must be subjected to safety audits independent of the design and operating groups, respectively.

3) Any information affecting safety, especially safety-related research results, must be subject to independent review, e.g., through a Technical Advisory Committee such as the one that audits AECL's program for fuel-waste management [17].

4) An institution applying for a licence must satisfy the regulator that it has, or has access to, appropriate technological support for safe operation.

5) A licensee must submit, for the regulator's approval, a list of signing authority for all important decisions in the design, commissioning, operation and decommissioning of the enterprise. All such decisions must be documented and properly authorized, and subjected to audit by the regulator. Except in an emergency, no action is permitted unless properly authorized.

To Both Regulatory Agency & Operating Utility

1) Responsibilities for safety audits and for reviewing any modifications to the design or to the operating procedures must be clearly defined.

2) The training and certification of personnel important to safety must be subject to regulatory approval.

To a large extent these suggested requirements would merely state explicitly in one place what is already accepted practice in Canada, but apparently not yet accepted everywhere. Making institutional QA (IQA) a formal requirement would, however, help to prevent the degeneration of existing institutions and assist any new institutions yet to be established. Furthermore, the existence of IQA would offer a reassurance to the public of continuing nuclear safety, in much the same way as enacting the Charter of Rights and Freedoms and repatriating the Constitution are seen as providing safeguards short of an absolute guarantee.

The ACNS concludes that the principles and methodology of quality assurance could and should be applied to the performance of institutions. While associating itself with the ONSR's endorsement of the safety of existing nuclear enterprises, the ACNS considers that some improvements are still possible and that the application of quality assurance to institutions could help to ensure continuing nuclear safety in the future.

4. PROPOSED MEASURES

The ACNS does not claim to have provided in this report a full description of institutional quality assurance (IQA), only to have identified the need for IQA and to have provided some examples of what it might include. What is needed first is a commitment to developing IQA, then identification of what should be included. Drafting standards for incorporation in Canadian nuclear standards, either as revisions to the existing ones or as separate ones applicable to institutional activities, would constitute a subsequent stage. The ultimate objective would be to include in AECB regulations appropriate requirements to protect against institutional failings.

Ideally, in the ACNS's view, the AECB should undertake the identification of what should be included in IQA. This task could be performed by AECB staff or on contract by a management consultant, either in the private sector or at a university. Other options are:

- To require a licence applicant to propose and implement an IQA program subject to AECB approval, or

- To encourage the Canadian Nuclear Association to undertake this initiative, as a further demonstration of the Canadian nuclear industry's wholehearted commitment to safety.

Whoever undertakes this task should assemble an advisory group consisting of representatives from all sectors of the nuclear industry, from the regulatory body, and from those who have experience in drafting standards for conventional QA.

One approach to tackling the problem would be to try to identify what is good in good institutions, what is bad in bad ones, and the differences between them. The principles and requirements developed in this way should be tested against the historical record, to see whether their application would have prevented past accidents and incidents, such as those noted in the appendices of this report. This check could lead to the identification of further requirements.

R.B. Maxwell [18], with extensive experience of quality assurance programs in both the nuclear and health-care industries, has suggested that the former may have something to learn from the latter in relation to IQA. Furthermore, a comparison between institutional attitudes to QA in non-nuclear industries in Canada and in Japan (where QA is generally regarded much more positively) could be profitable.

Whichever way IQA is initiated here, Canada should promote the concept at the IAEA, thereby continuing a long tradition of Canadian leadership in innovative measures for international nuclear safety. Canadian experience in this area could be invaluable to countries embarking on a nuclear program. Even on a level of self-interest, the Canadian nuclear industry cannot afford another Chernobyl anywhere.

The primary argument for IQA in nuclear energy is one of safety. However, there are two important spin-off benefits. Proponents of conventional QA claim that their programs more than pay for themselves; they provide large savings by avoiding costly faults. IQA would also be very useful in increasing public confidence in nuclear energy. Appreciation of these facts would help in gaining willing acceptance of IQA.

Despite all this, it must be recognized that IQA can improve safety but will not guarantee absolute safety. There is no such thing. It must be assumed that even with quality assurance in all its forms components will fail, human errors will occur and institutions will have failings. The Canadian approach to nuclear safety has assumed this from the start, and provided for it, largely through the defence-in-depth principle as explained in the ONSR Report [1].

In conclusion, the ACNS recommends that a methodology for institutional quality assurance (IQA) be developed and that the AECB initiate the development. The ultimate objective would be for the AECB to include the requirement for IQA in its regulations.

References

(1) Hare, Professor F. Kenneth, Commissioner, Ontario Nuclear Safety Review, "The Safety of Ontario's Nuclear Power Reactors". (1988)

(2) Advisory Committee on Nuclear Safety, "Recommendations and Comments on the Report of the Ontario Nuclear Safety Review", Report ACNS-15. (1988)

(3) Mosey, David & Weaver, Keith, "A Discussion of Institutional Failure and its Importance to Nuclear Safety", presented at the 1988 Annual Meeting of the Canadian Nuclear Society, Toronto. (1988)

(4) Penney, W., Schonland, B.F.J., Kay, J.M. & Diamond, J., "Report to the Chairman, UKAEA, on the Accident to the Windscale No. 1 Pile on October 10, 1957". (1957)

(5) Kemeny, John G., Chairman, The President's Commission on the Accident at Three Mile Island, "The Need for Change: The Legacy of TMI". (1979)

(6) Brooks, G.L. & Siddall, E., "An Analysis of the Three Mile Island Accident", Report AECL-7065. (1980)

(7) Atomic Energy Control Board, "The Accident at Chernobyl and its Implications for the Safety of CANDU Reactors", Report INFO-0234. (1987)

(8) Howieson, J.Q. & Snell, V.G., "Chernobyl - A Canadian Technical Perspective", Report AECL-9334. (1987)

(9) Ontario Hydro, "Submission to Ontario Nuclear Safety Review", (1987)

(10) Atomic Energy of Canada Limited, "A Submission to the Ontario Nuclear Safety Review", Report AECL-9427. (1987)

(11) Stevens, J.E.S. (AECL), Letter to Ms Margaret Grisdale (ONSR) dated 1987 July 13 with multiple attachments. (1987)

(12) Canadian Standards Association, "Quality Assurance Program Requirements for Nuclear Power Plants" (CAN 3-N286 Series).

(13) Atomic Energy Control Board, "Quality Assurance Programs for Nuclear Facilities", Consultative Document C-22. (1982)

(14) Advisory Committee on Nuclear Safety, "Recommended General Safety Requirements for Nuclear Power Plants", Report ACNS-4. (1983)

(15) International Atomic Energy Agency, "Basic Safety Principles for Nuclear Power Plants", IAEA Safety Series No. 75-INSAG-3. (1989)

(16) Advisory Committee on Nuclear Safety, "Assessment of IAEA Safety Series No. 75-INSAG-3 'Basic Safety Principles for Nuclear Power Plants'", Report ACNS-16. (1989)

(17) Shemilt, L.W., Chairman, Technical Advisory Committee on the Nuclear Fuel Waste Management Program, "Tenth Annual Report", Report TAC-10. (1989)

(18) Maxwell, R.B., private communication. (1989)

APPENDICES

Note: The highly simplified attributions of fault given in parentheses after items under each heading except "Institutional Failings" represent the ACNS's interpretation of what is said in the source documents. The items under the heading "Institutional Failings" represent ACNS judgements of such failings.

The attribution indicates the institution, not the individual, responsible, e.g., *"operating error"* indicates that the fault lay somewhere within the institution responsible for operation and maintenance.

A question mark (?) indicates that the attribution is uncertain due to inadequate information in the source document.

Appendix 1: US (Three Mile Island)

Sources: References (5) and (6)

Initiating Sequence:
- Resin blockage in feedwater polisher system (Design error)
- Water in air system (Operating error)
- Pilot-Operated Relief Valve (PORV) failed to close (Manufacturing error)

Primary Causes:
- Indicator lights misleading (Design error)
- Other Loss Of Coolant Accident (LOCA) indications ignored (Operating error)
- High pressure water injection cut back (Operating error)

Exacerbating Causes:
- Unprepared for hydrogen formation (Design error)
- Iodine filters misused (Operating error)
- Containment system leaks (Design error)

Contributing Causes:
- Condensate polishers faulty (Operating error)
- Emergency feedwater block valves closed, indicator not visible (Operating error)
- Controls, alarms & indicators confusing (Design error)
- Inadequate procedures (Operating error)
- Pipes/valves poorly identified (Operating error)

Underlying Causes:
- Preoccupation with regulations and the worst-case accident (Regulatory error)
- Operator training deficient (Regulatory/Operating error)
- Procedures confusing, poor practices (Operating error)
- Poor maintenance (Operating error)
- Utility weak in science & engineering; deficiencies in management, plant procedures, their implementation & surveillance, QA, audit and poor media briefing (Operating weakness)

- Lack of off-site emergency plan (Emergency Preparedness weakness)

- Regulatory inadequacies including the regulatory agency's structure, management, lack of operating experience, deficient inspection, surveillance & QA/QC; issues not resolved & retro-fitting not tackled; no systematic evaluation of experience; licensing ignores dual failures (Regulatory weakness)

Findings: The overall finding of the Kemeny Commission was that the fundamental problems were people-related, not equipment-related. Organizations, procedures, practices, but above all attitudes have to change. Although many detailed findings criticized the utility, just as many concerned the regulatory agency.

Institutional Failings:

- Continuation of operation with leaking PORV (Utility management)

- Failure to ensure that experience of a similar event, which was safely terminated, at another station was communicated to other utilities operating similar reactors (Regulatory agency)

- Failure of operating procedures to take into account effect of two-phase conditions in core on pressurizer level indications (Designer, utility management)

- Failures in procedures permitting operation with auxiliary feed-water line block-valves closed (Utility management)

- Inadequate procedures for accident conditions with poorly defined line of authority (Utility management, regulatory agency)

- Inadequate off-site emergency plan (Utility management, regulatory agency, state authorities)

- Regulatory inadequacies, as described under *"Underlying Causes"* (Regulatory agency)

- Utility weaknesses, as described under *"Underlying Causes"* (Utility management)

Appendix 2: USSR (Chernobyl)

Sources: - References (7) and (8)

Initiating Event: - Test conducted without proper review (Operating error)

Primary Causes:
- Operated reactor without adequate reactivity margin, contrary to regulation; operated reactor with almost all control rods withdrawn, in violation of operating policy (Operating error)
- Operated coolant flow above approved limit (Operating error)
- Emergency protection signals blocked, in violation of operating policy (Operating error)
- Ignored computer printout requiring immediate shut-down (Operating error)
- Reactor trip on turbogenerators blocked (Operating error)

Exacerbating Causes:
- Design unable to cope with large number of pressure tubes failing (Design weakness/Regulatory error)
- Areas above reactor vault outside containment (Design /Regulatory error)
- Very hot graphite caught fire when exposed, leading to most deaths and most release of radioactive material (Design vulnerability)
- Blanketed core without cooling to extinguish fire, causing much of the release (Emergency Preparedness weakness)

Contributing Causes:
- Commissioning test had been postponed (Regulatory error)
- Test procedures inadequately prepared (Operating error)
- Operators yielded to pressure to maintain production (Operating error)
- Setpoint adjustment overlooked (Operating error)
- Reactor shutdown system relatively slow, not independent of control system, not fully effective under all operating conditions, and capable of actually increasing reactivity on trip under conditions existing at the time of the accident (Design vulnerability)

Underlying Causes:

- Reactor design principles placed high reliance on correct operator action (Design vulnerability/Regulatory error)
- Reactor design vulnerable to accidents (Design vulnerability/ Regulatory error)
- Inadequate review & surveillance of non-routine operation (Operating/Regulatory error)
- Lack of emergency preparedness for unexpected accident (Emergency Preparedness weakness)

Comment:

- Our sources, eventually derived from USSR authorities, place primary blame on the operators. It would seem that this should be shared with the regulatory agency for lack of surveillance at least. Indeed, a case could be made that inadequacies on the part of the regulatory agency were the fundamental cause of the USSR accident.

Institutional Failings:

- Inadequate requirements for safety review of planned test (Regulatory agency, utility management)
- Failure to inculcate safety consciousness in operators (Utility management, regulatory agency)
- Procedures which permitted an external group to oversee and direct a planned test without apparent control by station management (Utility management, regulatory agency)
- Failure to recognize need for adequate containment and fully effective shut-down system (Designer, regulatory agency)
- Failure to recognize hazardous potential of safety absorber design (Designer, utility management, regulatory agency)
- Continued operation of reactor prior to accident with required safety-test not completed (Utility management, regulatory agency)
- Failure to recognize the importance of separation of control and safety functions (Designer, regulatory agency)
- Inadequate emergency procedures (State authorities, regulatory agency)

Appendix 3: CANDU Reactors (General)

Source: - Reference (11) [Att. = Attachment to letter]

Att. 13: Heat-transport-system depressurization, Bruce, 1975

- Human error during maintenance (Operating error), compounded by commissioning group's failure to communicate (Operating error) & spurious pump trip (Manufacturing error?)

Att. 14: Pressure-tube cracks, Pickering, 1974 & '83, Bruce '86

- Human error in installing rolled joints (Manufacturing error), compounded by inadequate inspection (QA failure) & failure to anticipate a failure mode (Design error)

- Human error in installing spacer springs (Manufacturing error), compounded by inadequate inspection (QA failure) & underestimate of deuterium pickup (Design error)

- Faulty tube fabrication (Manufacturing error), compounded by inadequate inspection (QA failure) & poor operating procedure for locating leak (Operating error)

Att. 16: Shutdown-cooling-system activated, Embalse, 1983

- Inadequate operating procedure for Shutdown Cooling System, plus minor inadequacies in other operating procedures (Operating error), initiated by feedwater interruption for unstated reason (Equipment failure?)

Att. 17: Loss of feed-water control, Embalse, 1983

- Water/dirt in air supply (Operating error), compounded by faulty programming of controller (Design & QA errors)

- Miscalculation in programming (Operating error)

Att. 18: Heavy-water spill, Wolsung, 1984

- 4 construction faults (Manufacturing errors) undetected (QA error), plus minor human error in maintenance (Operating error)

Att. 19: Follow-up investigation for previous incident

- Oversights in detailed design (Design & QA errors) plus reference to *"dormant failed open contacts"* (Operating error?)

Att. 20: Faulty liquid level indication in zone-control system, Bruce, 1984

- Equipment operated outside design limits (Operating error), plus lack of procedure to detect failure (Operating error) & possibly faulty instrument (Manufacturing error)

Att. 21: Dousing system initiated, Gentilly, 1985

- Apparently faulty procedure (Operating error)

Att. 22: Water hammer in emergency-core-cooling system, Embalse, 1986

- Incorrect wiring (Manufacturing error) undetected (QA error), initiated by human error in maintenance (Operating error); some deficiencies in operating according to procedures (Operating error)

Institutional Failings:

- For the burst pressure tube (Att. 14), the major institutional failing concerned a failure to anticipate and prevent movement of spacer springs and, as such, represented weaknesses in the QA programs (Designer, utility management, regulatory agency)

- For the Pickering and Bruce pressure tubes that leaked without bursting (Att. 14), the primary failing was of QA in manufacturing and installing the pressure tubes (Utility management responsible for construction)

- The causes of other incidents were largely human error at the individual level and weaknesses in the QA programs that did not constitute institutional failings as discussed in this report.

Acknowledgements

Members of the Working Group:

J.A.L. Robertson, Chairman

N.C. Lind

J.T. Rogers

N.L. Williams

Members of the Secretariat assisting:

R.J. Atchison

P. Smith (typing)

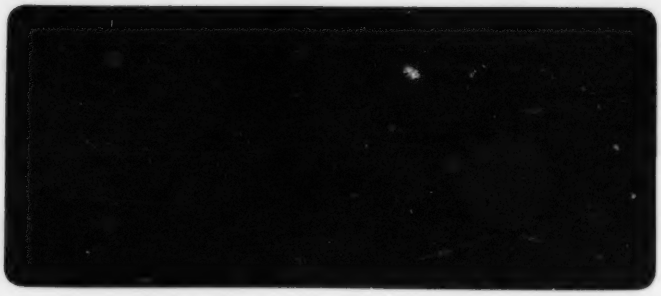
All the members of the Advisory Committee on Nuclear Safety.

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

Advisory Committees of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comités consultatifs de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9



COMMITTEE REPORTS

Since the 1950's the Atomic Energy Control Board has made use of advisory committees of independent experts to assist it in its decision-making process. In 1979 the Board restructured the organization of these consultative groups, resulting in the creation of two senior level scientific committees charged with providing the Board with independent advice on principles, standards and general practices related to radiation protection and the safety of nuclear facilities. The two committees are the Advisory Committee on Radiological Protection (ACRP), formed in 1979, and the Advisory Committee on Nuclear Safety (ACNS), which was established a year later. Summaries of meetings of the committees are available to the public in the AECB library in Ottawa.

From time to time the committees issue reports which are normally published by the AECB and catalogued within the AECB's public document system. Committee reports, bound with a distinctive cover, carry both a committee-designated reference number, e.g. ACRP-1, and an AECB reference number in the "INFO" series. The reports generally fall into two broad categories: (i) recommendations to the Board on a particular technical topic, and (ii) background studies. **Unless specifically stated otherwise, publication by the AECB of a committee report does not imply endorsement by the Board of the content, nor acceptance of any recommendations made therein.**

RAPPORTS DES COMITÉS

Depuis les années cinquante, la Commission de contrôle de l'énergie atomique fait appel à des comités consultatifs composés d'experts indépendants pour l'aider dans ses prises de décision. En 1979, la CCEA a restructuré l'organisation de ces groupes de consultation pour former deux comités scientifiques supérieurs chargés de lui fournir des conseils indépendants concernant les principes, les normes et les méthodes générales touchant la radioprotection et la sûreté des installations nucléaires : ce sont le Comité consultatif de la radioprotection (CCRP), formé en 1979, et le Comité consultatif de la sûreté nucléaire (CCSN), établi l'année suivante. Le public peut consulter les comptes rendus des réunions de ces comités à la bibliothèque de la CCEA, à Ottawa.

Les comités rédigent à l'occasion des rapports qui sont normalement publiés par la CCEA et catalogués dans la collection des documents publics de la CCEA. Reliés avec une couverture distincte, les rapports des comités se reconnaissent à leur numéro de référence du comité d'origine (comme CCRP-1) et à leur numéro de référence de la CCEA dans la série «INFO». Ils se divisent habituellement en deux catégories générales : (i) les recommandations présentées à la Commission au sujet d'une question technique particulière; (ii) les études générales. **À moins d'indication contraire, la publication par la CCEA du rapport d'un comité ne signifie pas que la Commission approuve le contenu de la publication, ni qu'elle en accepte les recommandations.**

Advisory Committees of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comités consultatifs de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

INFO-0359 (F)

ACNS Advisory Committee on Nuclear Safety

CCSN Comité consultatif de la sûreté nucléaire

CCSN-17

Amélioration de la culture de sûreté au sein des organisations : Proposition relative à l'assurance-qualité institutionnelle

par le

Comité consultatif de la sûreté nucléaire

février 1990

An Advisory Committee of the Atomic Energy Control Board of Canada — Secretariat: Ottawa, Canada K1P 5S9

Comité consultatif de la Commission de contrôle de l'énergie atomique du Canada — Secrétariat: Ottawa, Canada K1P 5S9

RÉSUMÉ

Les enquêtes sur les accidents graves, autant nucléaires que non nucléaires, qui se sont produits par le passé révèlent que ces accidents, en grande partie imputables à des erreurs humaines, témoignent également de défaillances au sein des institutions responsables. Bien qu'il soit reconnu que l'assurance de la qualité constitue un élément essentiel de tout procédé de production, les enquêtes menées jusqu'à maintenant n'ont jamais proposé d'appliquer ce principe aux institutions elles-mêmes. Le CCSN insiste sur l'importance de l'assurance-qualité institutionnelle, en donnant quelques exemples de ce qu'un tel principe suppose, et il propose des moyens pour y arriver.

Table des matières

	Page
RÉSUMÉ	i
Table des matières	ii
1. INTRODUCTION	1
2. DÉFAILLANCES INSTITUTIONNELLES	2
2.1 Approche	2
2.2 Graves accidents de réacteur	4
2.2.1 Windscale (Royaume-Uni)	4
2.2.2 Three Mile Island (États-Unis)	4
2.2.3 Tchernobyl (Union soviétique)	5
2.3 Réacteurs CANDU	6
2.4 Conclusion	6
3. RÔLE PROGRAMME D'ASSURANCE-QUALITÉ	7
4. MESURES PROPOSÉES	11
Références	13
ANNEXES	15
Annexe 1	1-1
Annexe 2	2-1
Annexe 3	3-1
Remerciements	

1. INTRODUCTION

Ceux qui se préoccupent de la sûreté nucléaire prennent de plus en plus conscience de l'importance de la "culture de sûreté" au sein des institutions engagées dans des activités nucléaires. Bien que l'on ne s'entende pas encore sur la définition précise de cette notion, la plupart des gens connaissent des institutions dont les membres se soucient davantage de la sûreté que d'autres.

F.K. Hare, Commissaire du Ontario Nuclear Safety Review (ONSR), a consacré une section entière de son rapport à la culture de sûreté chez Ontario Hydro ("Ontario Hydro Safety Culture") [1]. En voici un extrait :

> (traduction libre)
> *"Nul ne peut douter de l'importance que Ontario Hydro accorde au maintien de la sûreté. Il est toutefois un aspect dont la société ne discute pas en profondeur; je veux parler de la "culture de sûreté" au sein de cette société, expression utilisée par les ingénieurs industriels pour désigner toute l'atmosphère qui entoure le maintien de la sûreté, tant de façon officielle qu'officieuse. Pour utiliser le jargon d'aujourd'hui, le programme caché de sûreté influe également sur les résultats, peut-être même de façon décisive."*

Il soulève un peu plus loin les questions suivantes :

> *"Comment une grande société peut-elle s'assurer que ses normes rigoureuses actuelles seront maintenues, voire améliorées? Comment Ontario Hydro peut-elle arriver à cette fin? Il ne s'agit pas ici de questions rhétoriques. En effet, d'autres exploitants ont vu leurs compétences s'effriter tout comme des sociétés privées se sont dégradées sans raison apparente... Cela pourrait-il arriver également à Ontario Hydro?"*

Dans son rapport CCSN-15 [2], le Comité consultatif de la sûreté nucléaire de la Commission de contrôle de l'énergie atomique commente le rapport du ONSR et formule plusieurs recommandations pertinentes. L'une d'entre elles (n° 6) se lit comme suit :

> *"Le CCSN recommande que la CCEA appuie des études sur les éléments d'une "culture de sûreté" solide, afin de pouvoir déceler toute faiblesse au sein des organisations dans ce domaine."*

En ce qui a trait au choix de l'approche visant à assurer une culture de sûreté solide, le CCSN fait référence à un autre extrait du rapport du ONSR [1] :

> (traduction libre)
> *"Dans un examen des mémoires présentés au ONSR, J.A.L. Robertson (faisant part de commentaires personnels à titre d'expert-conseil)* soutient avec insistance que le maintien de la qualité dans le fonctionnement des institutions est aussi important pour la sûreté que ne l'est l'assurance-qualité matérielle."*

---

* Nommé depuis au sein du CCSN.

En conséquence, le CCSN a entrepris une étude ayant pour objectifs :

- de déterminer si les défaillances des institutions, par opposition aux défectuosités des composants et aux erreurs humaines, ont contribué de façon significative à des accidents de réacteurs et à des événements imprévus (désignés "événements importants" par Ontario Hydro);

- de déterminer si les principes et les méthodes liés à l'assurance-qualité peuvent être appliqués ou adaptés de manière à réduire la probabilité de défaillances institutionnelles futures, et

- le cas échéant, d'indiquer quelles initiatives pourraient être entreprises, et par qui elles devraient l'être, pour la mise en oeuvre d'un programme d'assurance-qualité institutionnelle pour l'énergie nucléaire.

Chacun de ces trois objectifs est étudié plus en détail dans les sections qui suivent.

2. DÉFAILLANCES INSTITUTIONNELLES

2.1 Approche

Les accidents constituent la manifestation la plus flagrante des lacunes au niveau de la sûreté. Dans la plupart des cas, les enquêtes sur les accidents révèlent que ceux-ci sont imputables à une ou plusieurs des trois causes générales suivantes : erreur de conception, défaillance d'un composant ou erreur humaine.

On s'est toutefois rendu compte que la désignation "erreur humaine" ne décrivait pas toujours adéquatement les erreurs auxquelles étaient associées des personnes. Trop souvent, la cause sous-jacente de l'accident tient au fait que l'institution à laquelle appartiennent les personnes en cause n'a pas su établir ou prendre des précautions adéquates en matière de sûreté. Voilà ce qu'on entend par défaillances institutionnelles.

Mosey et Weaver font référence à cette cause d'accidents dans leur mémoire présenté lors de l'assemblée annuelle de 1988 de la Société nucléaire canadienne [3]. Dans ce document intitulé "A Discussion of Institutional Failure and its Importance to Nuclear Safety", ils examinent et analysent les causes de huit accidents. Ils en viennent à la conclusion suivante :

> (traduction libre)
> *"Il semble que la défaillance institutionnelle soit en cause dans une proportion significative de ces accidents ..., cette notion voulant désigner l'absence de certaines fonctions nécessaires ou souhaitables pour le maintien de la sûreté, ou leur incapacité de satisfaire à des critères minimums de sûreté."*

Les auteurs insistent sur la nécessité de mieux définir la notion de défaillance institutionnelle.

De son côté, le CCSN a adopté la définition suivante :

> **Dans le contexte de la sûreté nucléaire, "défaillance institutionnelle" désigne un manquement à la sûreté dont la cause, au sein de l'institution concernée, va au-delà de l'agent immédiat, qu'il s'agisse d'une défaillance matérielle ou d'une erreur humaine.**

Les défaillances institutionnelles ne se limitent toutefois pas à l'industrie nucléaire, loin de là. À titre d'exemple, une enquête effectuée après l'écrasement d'un avion aux États-Unis a révélé que l'équipage n'effectuait pas toujours les vérifications prescrites avant le décollage et qu'il pouvait arriver qu'il mette certains instruments de vol hors circuit. De même, après l'écrasement du vol n° 655 de la compagnie Iran Air, qui a été abattu par la flotte américaine, on a appris que les pilotes de cette ligne aérienne passaient souvent outre aux demandes d'identification provenant de la marine américaine. L'enquête menée au Royaume-uni sur l'incendie désastreux qui s'est produit dans la station de métro King's Cross a jeté le blâme sur les hauts fonctionnaires de la Société de transports de Londres qui ont omis de voir à l'adoption de mesures de protection adéquates en sachant que d'autres incendies de nature similaire s'étaient déjà produits. À la suite du déversement de pétrole provoqué par l'accident du Exxon Valdez en Alaska, le test effectué sur le capitaine du superpétrolier, souffrant semble-t-il d'un problème d'alcoolisme, a révélé que le taux d'alcool dans le sang de ce dernier était supérieur aux normes prescrites par la loi; on a également appris que la personne qui occupait le poste d'officier de quart n'avait pas été accréditée pour naviguer dans ces eaux. Enfin, au Canada, l'enquête sur l'effondrement d'un supermarché le jour de son ouverture a révélé que le toit n'avait pas été construit correctement et a mis en lumière des lacunes institutionnelles au sein de la firme d'ingénierie affectée au projet de même qu'au sein de l'organisme de réglementation.

Ce qui est le plus inquiétant, c'est que dans tous ces cas les infractions étaient, semble-t-il, de notoriété publique, mais que rien, ou presque rien, n'a été fait par les institutions concernées. Il ne faut donc pas s'étonner que le public ne se fasse plus d'illusions au sujet des prétendues précautions de sûreté prises à l'égard de nombreuses technologies. De plus en plus, nous entendons des remarques du genre : "Le système a fait défaut", "On nous avait dit que cela ne pouvait pas arriver", ou "Pourquoi devrions-nous vous faire confiance maintenant?"

Le CCSN reconnaît que ces rapports non confirmés publiés dans les médias ne constituent pas la preuve que la défaillance institutionnelle est devenue un problème répandu. Ils portent toutefois à croire que ce problème pourrait être une cause d'accident qui ne reçoit pas toute l'attention voulue. Le CCSN a donc voulu déterminer s'il existait des cas de défaillance institutionnelle prouvée dans le domaine nucléaire. Il a pour ce faire passé en revue les rapports d'enquête sur des accidents nucléaires antérieurs, ces rapports constituant les études les plus complètes et les mieux documentées sur les causes des défaillances liées à la sûreté. Les trois accidents étudiés ont été choisis en raison de leur pertinence par rapport aux critères suivants :

- lien avec les réacteurs de puissance (puissance relativement élevée);

- incidence sur la sécurité publique (libération réelle ou potentielle de substances radioactives);

- disponibilité de documentation;

- importance des résultats pour le public (sensibilisation du public à l'accident).

Comme aucun de ces trois accidents ne s'est produit au Canada, le CCSN a approfondi son étude sur les défaillances institutionnelles en examinant les rapports sur les incidents les plus graves impliquant des réacteurs CANDU.

2.2 Graves accidents de réacteurs

2.2.1 Windscale (Royaume-Uni)

Le 10 octobre 1957, le combustible en uranium métallique et le ralentisseur au graphite de l'un des réacteurs plutonigènes à Windscale, au Royaume-Uni, prenaient feu à la suite d'une période d'exploitation à faible puissance prévue durant l'entretien du réacteur. En l'absence de pratiquement toute enceinte de confinement, au sens où nous l'entendons maintenant, de grandes quantités de substances radioactives ont été libérées et se sont propagées à travers le Royaume-Uni et dans plusieurs pays d'Europe du Nord. Bien que cet accident n'ait provoqué immédiatement ni mort ni blessure, les substances libérées pourraient avoir causé une certaine augmentation du nombre de cas de cancer dans les régions touchées.

Un comité chargé de faire enquête sur l'accident faisait part de ses conclusions [4] un peu plus tard au cours du même mois. Selon Mosey et Weaver [3] :

> (traduction libre)
> *"Selon le Comité, la principale défectuosité technique à l'origine de l'accident vient du caractère inadéquat de l'instrumentation qui n'a pu assurer une exploitation "sécuritaire et adéquate" d'un déclenchement Wigner. Le Comité a par ailleurs indiqué que l'absence quasi complète de documents de fonctionnement constituait une "grave lacune" et il a souligné un certain nombre de "lacunes et de défaillances" au niveau de l'organisation, notamment le fait que le partage des responsabilités est insuffisamment defini et que l'on se fie trop à des comités pour assurer la direction technique. Il a aussi insisté sur le manque de soutien technique offert aux employés affectés aux opérations à Windscale..."*

2.2.2 Three Mile Island (États-Unis)

Le 28 mars 1979, une perte de caloporteur dans le réacteur n^{o} 2 (réacteur à eau sous pression) de la centrale nucléaire de Three Mile Island, en Pennsylvanie (États-Unis), provoquait la fusion partielle du coeur du réacteur. En dépit de la gravité des dommages physiques causés au réacteur, la presque totalité des matières radioactives ont été retenues à l'intérieur de l'enceinte de confinement. Selon les estimations, les faibles quantités de substances radioactives qui se sont échappées représentaient, pour les membres du public les plus exposés, des doses de rayonnement à peu près équivalentes aux doses annuelles reçues de sources naturelles (rayonnement naturel).

Le rapport présenté au Président des États-Unis par la Commission qui, sous la présidence de John G. Kemeny [5], était chargée de faire enquête sur l'accident à Three Mile Island, fait état de lacunes dans la conception et dans les composants de la centrale, ainsi que d'erreurs de la part des opérateurs; il souligne également un grand nombre de lacunes dans les institutions concernées. De l'avis du CCSN, les principales causes de l'accident sont imputables à l'exploitant et à l'organisme de réglementation; il s'agit donc en d'autres termes de défaillances institutionnelles. Bon nombre des recommandations formulées dans le rapport traitent de ces lacunes.

L'annexe 1 présente un résumé des causes de cet accident. Lorsqu'on examine ces causes en détail, on constate que bon nombre d'entre elles ne sont pas imputables à des individus (opérateurs, concepteurs, etc.), mais plutôt aux institutions pour lesquelles travaillaient ces personnes. Qui plus est, l'existence d'un si grand nombre de lacunes en même temps laisse croire fortement à des lacunes au sein des institutions concernées, de l'organisme chargé de la conception des installations, de l'organisme exploitant et de l'organisme de réglementation. Les lacunes institutionnelles qui, de l'avis du CCSN, ont contribué à l'accident sont indiquées sous la rubrique "Défaillances institutionnelles" dans cette annexe et dans les annexes suivantes.

2.2.3 Tchernobyl (Union soviétique)

Le pire accident de réacteur au monde s'est produit à Tchernobyl, en Ukraine (Union soviétique), le 26 avril 1986. À la suite de tests effectués par les opérateurs sur le réacteur 4 (réacteur de type RBMK, modéré au graphite et refroidi à l'eau) durant le processus d'arrêt du réacteur, une instabilité s'est developpée dans le contrôle : la puissance a augmenté soudainement pour atteindre un niveau près de cent fois le niveau de pleine puissance. Ceci a provoqué des explosions chimiques et le graphite a pris feu; il y a eu ensuite destruction du coeur du réacteur et de son bâtiment et éjection de fragments en combustion dans les zones avoisinantes. Le reste du graphite a continué de brûler pendant plus de dix jours. L'incendie a été un des principaux facteurs contribuant à la mort de 31 personnes qui faisaient partie des employés de la centrale ou de l'équipe d'intervention d'urgence et qui sont mortes des suites directes de l'explosion, des rayonnements ou de l'incendie; l'incendie a également provoqué la propagation de substances radioactives sur la majeure partie de l'Europe, ce qui risque d'accroître de quelques milliers le nombre de morts additionnelles par cancer au cours des cinquante prochaines années (ce nombre représente toutefois une proportion bien inférieure à un pour cent des morts par cancer susceptibles d'être provoquées par l'ensemble des autres causes).

Une rencontre subséquente au sujet de l'accident de Tchernobyl [7,8], qui s'est tenue à Vienne sous l'égide de l'Agence internationale de l'énergie atomique (AIEA), a fait ressortir certaines lacunes fondamentales dans la conception du réacteur; l'impression générale retenue cependant était celle d'une combinaison d'erreurs des opérateurs et d'inconduite que l'on aurait cru impensables si cet accident ne s'était pas réellement produit. Les autorités soviétiques jettent le blâme sur les opérateurs concernés et sur la direction de la centrale. Cependant, ceux qui, au Canada, connaissent bien ce genre d'entreprise ne peuvent expliquer cette séquence d'événements autrement que par l'existence de graves lacunes au sein des institutions soviétiques concernées, de l'exploitant et de l'organisme de réglementation. Pour des raisons que nous ne pouvons pas

encore comprendre parfaitement, ces institutions n'ont pas pris les mesures nécessaires pour éviter que des infractions aussi graves ne soient commises. L'AIEA, en évitant d'attirer l'attention sur ces lacunes au sein des institutions, a fait preuve elle aussi de défaillance institutionnelle. Or, d'ici à ce que toutes ces lacunes soient identifiées et corrigées, il sera impossible de croire, en toute confiance, que pareil accident ne pourra se reproduire. L'annexe 2 fournit des justifications sur les conclusions formulées dans le présent paragraphe.

2.3 Réacteurs CANDU

Le pire accident dans un réacteur canadien CANDU s'est produit le 1er août 1983. Un tube de force du réacteur 2 de la centrale de Pickering-A s'est rompu alors que le réacteur fonctionnait à pleine puissance. Les opérateurs ont alors arrêté le réacteur en suivant le processus normal, c'est-à-dire sans avoir besoin de faire appel à un seul système de sûreté. Aucun employé de la centrale n'a été blessé et aucun matériau radioactif ne s'est échappé de la centrale; les réparations ont toutefois été coûteuses sur le plan économique.

Une enquête subséquente sur l'incident [9,10] a révélé que les assemblages des canaux de combustible ne se trouvaient pas dans la configuration prévue dans les plans car il n'y avait aucune disposition concernant l'emplacement exact des ressorts d'écartement entre les tubes de force et les tubes de calandre. Les ressorts n'étaient donc pas aux endroits où ils auraient dû être et il y avait contact entre les deux tubes. La cause apparente de l'incident est donc une lacune au niveau de la conception, aggravée par la mise en place d'un programme d'assurance-qualité inadéquat pour les phases de construction et de mise en service.

Cependant, l'élément le plus pertinent dans le contexte actuel est que les institutions concernées disposaient de toute l'information nécessaire pour prévenir la rupture des tubes de force, mais qu'elles ont négligé de coordonner et d'évaluer l'information disponible, et de prendre les mesures qui s'imposaient. Bien que ces lacunes au sein des institutions n'aient porté atteinte ni à la sécurité du public ni à celle des employés, leurs conséquences ont cependant été fort coûteuses.

Énergie atomique du Canada Limitée (EACL) a présenté au ONSR un dossier [11] faisant état des plus graves incidents impliquant des réacteurs CANDU, y compris l'incident précité. Bien que ce rapport ne conclue pas à des défaillances institutionnelles aussi graves que celles observées à Windscale, Three Mile Island et Tchernobyl, il s'impose d'améliorer le programme d'assurance-qualité conventionnelle. L'annexe 3 fournit des détails à ce sujet.

2.4 Conclusion

Après examen des accidents de réacteurs précités et d'autres qui n'ont pas été décrits dans le présent document, le CCSN en vient à la conclusion que les défaillances institutionnelles ont en fait contribué de façon significative aux manquements à la sûreté nucléaire qui se sont produits à l'extérieur du Canada. Il conclut également que, bien que le bilan du Canada dans ce domaine soit en général satisfaisant, certaines améliorations seraient souhaitables concernant le fonctionnement des institutions.

3. RÔLE DU PROGRAMME D'ASSURANCE-QUALITÉ

Même si le CCSN corrobore la conclusion du commissaire du ONSR [1] selon laquelle :

> (traduction libre)
> " *Les réacteurs de Ontario Hydro sont exploités de façon sécuritaire et répondent à des normes rigoureuses en matière de rendement technique*",

il partage également les préoccupations exprimées par le commissaire qui craint que les normes rigoureuses actuelles puissent ne pas être maintenues à l'avenir.

Ainsi, des institutions qui jouissaient auparavant d'une excellente réputation, comme les sociétés ferroviaires et les services postaux, se sont détériorées en un laps de temps court par rapport à la durée de vie prévue des réacteurs. Les préoccupations exprimées ne reposent pas uniquement sur le processus normal de vieillissement des institutions, mais également sur les problèmes organisationnels inhérents à une institution qui connaît une croissance rapide ou qui fait face à une décroissance. Les institutions publiques sont également sensibles aux pressions politiques qui, bien que louables en soi, peuvent entrer en conflit avec les responsabilités d'une institution en matière de sûreté.

Le CCSN a donc examiné les méthodes qui sont actuellement disponibles ou qui pourraient être mises au point pour éviter les défaillances institutionnelles et ainsi maintenir, voire améliorer, le bilan actuel des institutions canadiennes en matière de sûreté. Il en résulterait également un autre avantage du fait que le public aurait davantage confiance en la sûreté des réacteurs CANDU, en étant mieux renseigné sur les mesures prises en vue de prévenir toute défaillance de la part des institutions.

Comme l'assurance-qualité s'est avérée un moyen très efficace pour réduire la fréquence des défauts de fabrication, nous en avons examiné l'application au fonctionnement des institutions.

La discipline de l'assurance-qualité découle principalement des programmes militaires et aérospatiaux américains, où les conséquences de défectuosités peuvent être réellement catastrophiques. Aujourd'hui, toutefois, l'ensemble de l'industrie prend de plus en plus conscience des avantages économiques liés à l'assurance-qualité. À titre d'exemple, la société Ford mise aujourd'hui sur la "Qualité avant tout".

Dans le présent document, assurance-qualité se définit comme suit (il ne s'agit toutefois pas d'une définition retenue universellement par les praticiens d'assurance-qualité) :

> **L'assurance-qualité désigne le regroupement de tous les moyens requis pour s'assurer, avec un haut niveau de confiance, que la qualité de tous les composants d'une entreprise soit conforme à l'objectif pour lequel ceux-ci ont été conçus, de manière à ce que l'ensemble de l'entreprise puisse produire le rendement escompté. Les composants incluent les matériaux, la conception, la fabrication, la construction, les modes d'exploitation, le comportement humain et le rendement de l'ensemble de l'institution; cette**

liste n'est toutefois pas exhaustive. La vérification est en outre un élément essentiel de tout programme d'assurance-qualité et elle doit être indépendante des structures directement responsables des diverses composantes de l'entreprise.

Cette définition comporte une notion importante, selon laquelle il n'est pas nécessaire d'exiger la plus haute qualité pour chaque composant; il s'agit plutôt d'obtenir une qualité qui convienne à l'usage prévu. Dans le même ordre d'idées, un programme d'assurance-qualité doit être approprié. Le fait d'insister sur la mise en oeuvre d'un programme excessif et non justifié ne fera que soulever des résistances.

Nous soulignons dans le présent rapport les avantages que l'assurance-qualité présente sur le plan de la sûreté. D'autres prétendent que les avantages économiques constituent la principale motivation et qu'il faut accepter les programmes d'assurance-qualité avec enthousiasme et ne pas s'y opposer à cause des coûts supplémentaires, imposés de l'extérieur, qu'ils occasionnent. Ces deux points de vue sont probablement valables, l'équilibre entre la sûreté et les avantages économiques variant d'une industrie à l'autre.

L'industrie nucléaire canadienne reconnaît la nécessité et la valeur de l'assurance-qualité. L'Association canadienne de normalisation a élaboré une série de normes intitulées "Exigences relatives au programme d'assurance-qualité des centrales nucléaires"[12]. Ces normes couvrent bon nombre des points précis soulevés dans le présent rapport, bien qu'elles semblent, en pratique, être appliquées presque entièrement au niveau de l'exécution. De plus, ces normes ne s'appliquent pas à l'organisme de réglementation, même s'il s'agit d'une des institutions les plus importantes dans le domaine de la sûreté nucléaire et même si cet organisme, dans les exemples étudiés par le CCSN pour d'autres pays (section 2), a déjà fait preuve de défaillances.

La CCEA exige l'élaboration et la mise en vigueur d'un programme efficace d'assurance-qualité pour chaque installation nucléaire et elle a établi des exigences à cet effet dans son document de consultation C-22 [13]. De son côté, le CCSN a défini, dans son rapport CCSN-4 "Exigences générales de sûreté recommandées pour les centrales nucléaires" [14], les exigences relatives à l'établissement d'un programme d'assurance-qualité approprié dans les domaines de la conception et de la construction. De même, le rapport du ONSR [1] et le rapport "Basic Safety Principles for Nuclear Power Plants" [15] de l'AIEA définissent l'assurance-qualité comme un des éléments les plus importants sur lesquels repose la sûreté nucléaire. Enfin, dans son étude du document de l'AIEA, le CCSN (rapport CCSN-16 [16]) souligne que l'AIEA insiste davantage sur la culture de sûreté que ne le fait le CCSN dans son rapport CCSN-4 et il souscrit à cette approche de l'AIEA.

Après examen de la documentation existante, il devient évident qu'un grand nombre des éléments devant constituer un programme d'assurance-qualité global ont déjà été identifiés par l'industrie nucléaire canadienne et son organisme de réglementation. Cependant, bien que les principes et les exigences s'appliquent aux employés des institutions concernées, aucun programme d'assurance-qualité officiel et intégré ne s'applique aux institutions elles-mêmes. Cette omission est particulièrement importante, compte tenu du fait que les défaillances institutionnelles sont, de façon plus ou moins importante, responsables des accidents qui se sont produits à Three Mile Island et à Tchernobyl.

En examinant de quelle façon l'assurance-qualité pourrait être appliquée aux institutions, le CCSN a d'abord défini quelques-uns des plus importants principes de cette discipline. Ils sont énumérés ci-après (par ordre alphabétique), en fonction de leur application aux institutions :

Autorisation	Les institutions doivent s'assurer qu'aucune activité ne sera entreprise sans avoir reçu au préalable les autorisations nécessaires.
Capacité d'être retracé	Toutes les chaînes de responsabilité et de raisonnement au sein d'une institution doivent pouvoir être clairement retracées.
Évaluation	Les systèmes de gestion des institutions doivent prévoir des mécanismes pour mesurer leur rendement.
Imputabilité	Les institutions, de même que les personnes, doivent rendre compte de leurs actions.
Indépendance	La vérification et la réglementation doivent être faites par des personnes, des groupes ou des institutions indépendants, du point de vue organisationnel, de ceux qui sont responsables de la mise en oeuvre des activités visées.
Intégrité	Toute information utilisée par une institution et susceptible d'avoir des répercussions sur la sûreté doit être hautement fiable.
Responsabilité	Les responsabilités, ainsi que le partage des responsabilités, doivent être clairement définis au sein de l'institution.
Vérification	Le dossier de fonctionnement de toute institution susceptible d'avoir des répercussions sur la sûreté doit faire l'objet d'une vérification.
Visibilité	L'ensemble du procédé doit être aussi ouvert que possible à l'inspection par le public.

Voici quelques façons dont ces principes pourraient être appliqués aux institutions dans le domaine nucléaire :

Organisme de réglementation

1) Dans la mesure du possible, la fonction de réglementation au sein du système gouvernemental canadien doit être indépendante des autres fonctions, p. ex. conception, recherche et développement, promotion, commercialisation et exploitation.

2) L'organisme de réglementation doit faire une distinction entre politiques, règlements et directives et les définir chacun en termes clairs et précis.

3) L'élaboration des politiques, des règlements et des directives par l'organisme de réglementation doit se faire selon un processus qui permet aux parties intéressées d'y participer; on n'a qu'à penser par exemple aux documents de consultation qu'utilise actuellement la CCEA. Les commentaires formulés, et le traitement qui en est fait avec raisons à l'appui, doivent également être documentés.

4) L'organisme de réglementation doit définir les exigences et les objectifs de façon à ce qu'ils puissent être évalués, de préférence en des termes quantitatifs : ainsi, une exigence dont on ne pourrait vérifier à quel point elle est satisfaite n'aurait guère d'utilité.

5) L'organisme de réglementation doit noter et étayer ses décisions, avec raisons explicites à l'appui.

6) L'organisme de réglementation doit vérifier le fonctionnement des titulaires de permis.

7) Autant de documentation que possible doit être accessible au public, y compris les commentaires formulés à l'égard des documents de consultation et les résumés des vérifications du fonctionnement des détenteurs de permis.

Organisme exploitant

1) L'institution qui présente une demande de permis doit soumettre à l'approbation de l'organisme de réglementation des programmes d'assurance-qualité couvrant tous les aspects des activités de l'entreprise; ces programmes devront en outre faire l'objet d'une vérification par l'organisme de réglementation.

2) La conception ainsi que toutes les procédures d'exploitation doivent être soumises à des vérifications de sûreté effectuées par des groupes ou des personnes indépendants respectivement des groupes affectés à la conception et à l'exploitation.

3) Toute information concernant la sûreté, en particulier les résultats de recherches liées à la sûreté, doit faire l'objet d'un examen indépendant par l'entremise, par exemple, d'un comité technique consultatif comme celui chargé de vérifier le programme de EACL sur la gestion des déchets de combustible nucléaire [17].

4) Toute institution qui fait une demande de permis doit convaincre l'organisme de réglementation qu'elle dispose d'un soutien technologique approprié pour assurer la sûreté de l'exploitation ou qu'elle a accès à un tel soutien.

5) Le titulaire de permis doit soumettre à l'approbation de l'organisme de réglementation une liste des fondés de signature pour toutes les décisions importantes touchant la conception, la mise en service, l'exploitation et le déclassement de l'entreprise. Toutes ces décisions doivent être documentées et dûment autorisées et faire l'objet d'une vérification par l'organisme de réglementation. Sauf en cas d'urgence, aucune activité ne pourra être entreprise à moins d'avoir reçu les autorisations nécessaires.

Organisme de réglementation et organisme exploitant

1) Les responsabilités concernant les vérifications de sûreté, ainsi que l'examen de toute modification à la conception ou aux procédures d'exploitation, doivent être clairement définies.

2) Les programmes de formation et d'accréditation des employés ayant un rôle important à jouer dans le maintien de la sûreté doivent être soumis à l'approbation de l'organisme de réglementation.

L'adoption des exigences proposées ci-haut ne ferait dans une large mesure que définir explicitement ce qui est déjà pratique courante au Canada, mais qui ne semble pas encore accepté partout. Cependant, faire de l'assurance-qualité institutionnelle une exigence officielle aiderait à prévenir la dégradation des institutions existantes et faciliterait l'établissement des nouvelles institutions. De plus, l'existence de tels programmes permettrait de rassurer le public quant au maintien de la sûreté nucléaire, de la même façon que l'adoption de la Charte des droits et des libertés et le rapatriement de la Constitution sont perçus comme des protections, à défaut d'une garantie absolue.

Le CCSN conclut que les principes et les méthodes de l'assurance-qualité peuvent et doivent s'appliquer au fonctionnement des institutions. Par ailleurs, bien que le CCSN corrobore l'opinion du ONSR quant à la sûreté des entreprises nucléaires existantes, il estime néanmoins que des améliorations pourraient être apportées et que l'application de l'assurance-qualité aux institutions pourrait aider à assurer à l'avenir le maintien de la sûreté nucléaire.

4. MESURES PROPOSÉES

Le CCSN ne prétend pas avoir donné, dans le présent rapport, une description exhaustive de l'assurance-qualité institutionnelle; il a plutôt voulu souligner la nécessité d'un tel programme et présenter quelques exemples de ce qu'un tel programme pourrait inclure. Il faut avant tout prendre un engagement à l'égard de l'assurance-qualité institutionnelle; les modalités de ces programmes pourront ensuite être définies. L'élaboration de normes qui seraient incluses dans les normes nucléaires canadiennes, sous forme, soit de révisions des normes actuelles, soit de normes distinctes applicables aux activités des institutions, constitue une étape subséquente. L'objectif ultime serait d'inclure dans les règlements de la CCEA des exigences pertinentes pour prévenir toute défaillance de la part des institutions.

Idéalement, estime le CCSN, la CCEA devrait se charger de définir les éléments à inclure dans les programmes d'assurance-qualité institutionnelle. Cette tâche pourrait être confiée au personnel de la CCEA ou à des experts-conseils du secteur privé ou du milieu universitaire, engagés sur une base contractuelle. Parmi les autres options qui s'offrent, mentionnons les suivantes :

- Exiger de la part du demandeur de permis l'élaboration et la mise en oeuvre d'un programme d'assurance-qualité institutionnelle soumis à l'approbation de la CCEA, ou

- Encourager l'Association nucléaire canadienne à s'acquitter de cette tâche, afin de démontrer une fois de plus l'intérêt véritable que porte l'industrie nucléaire canadienne à la sûreté.

Quiconque s'acquittera de cette tâche devra mettre sur pied un groupe consultatif composé de représentants de tous les secteurs de l'industrie nucléaire, de l'organisme de réglementation et des organismes avec expérience dans l'élaboration de normes relatives à l'assurance-qualité conventionnelle.

Une approche qui pourrait être utilisée pour mener à bien cette tâche serait de tenter de déterminer les éléments positifs des bonnes institutions et les éléments négatifs des mauvaises institutions, et de faire ressortir les différences entre les deux. Les principes et les exigences qui seraient définis de cette façon seraient ensuite éprouvés, pour voir si leur application aurait permis de prévenir les accidents et incidents antérieurs, comme ceux qui sont décrits dans les annexes ci-jointes. Cette vérification pourrait également permettre de définir d'autres exigences.

R.B. Maxwell [18], qui possède une vaste expérience des programmes d'assurance-qualité, tant dans l'industrie nucléaire que dans le secteur de la santé, a indiqué que l'industrie nucléaire pourrait sans doute en apprendre du secteur de la santé en matière d'assurance-qualité institutionnelle. Il pourrait en outre être profitable d'établir une comparaison entre les attitudes des institutions du Canada et du Japon (où l'assurance-qualité est en général perçue de façon beaucoup plus positive) à l'égard de l'assurance-qualité dans les industries non nucléaires.

Quelle que soit l'approche que nous choisirons pour la mise en oeuvre des programmes d'assurance-qualité institutionnelle, le Canada devrait également en promouvoir le concept auprès de l'AIEA, afin de demeurer fidèle à sa réputation de longue date de chef de file dans le domaine des mesures innovatrices en matière de sûreté nucléaire internationale. L'expérience du Canada dans ce domaine pourrait être d'une valeur inestimable pour les pays qui se lancent dans un programme nucléaire. Même si ce n'est que pour protéger ses propres intérêts, l'industrie nucléaire canadienne ne peut se permettre qu'un accident comme celui de Tchernobyl se répète ailleurs.

La sûreté est bien sûr le principal argument qui milite en faveur de l'application de programmes d'assurance-qualité institutionnelle dans le secteur de l'énergie nucléaire. Il découle toutefois de ces programmes deux autres avantages importants. Ainsi, les tenants des programmes d'assurance-qualité conventionnelle prétendent que les avantages qui résultent de ces programmes sont bien supérieurs aux coûts qu'ils occasionnent; ils permettent en effet de réaliser des économies substantielles en prévenant les défaillances coûteuses. En outre, les programmes d'assurance-qualité institutionnelle seraient très utiles pour accroître la confiance du public à l'égard de l'énergie nucléaire. L'appréciation de ces faits aiderait à faire accepter l'assurance-qualité institutionnelle.

En dépit de tout cela, il faut reconnaître que l'assurance-qualité institutionnelle peut améliorer la sûreté, mais qu'elle ne constitue pas une garantie absolue de sûreté. Cela n'existe pas. Il faut en effet présumer qu'en dépit de l'application d'une gamme complète de programmes d'assurance-qualité, il continuera d'y avoir défaillances techniques, erreurs humaines et défaillances institutionnelles. L'approche canadienne en matière de sûreté nucléaire a été fondée dès le départ sur cette hypothèse et elle en a tenu compte, principalement par le biais du principe de défense en profondeur tel qu'expliqué dans le rapport du ONSR [1].

En conclusion, le CCSN recommande que la CCEA amorce l'élaboration d'une méthodologie relative à l'assurance-qualité institutionnelle. L'objectif ultime serait qu'une exigence en ce sens soit incluse dans les règlements de la CCEA.

Références

(1) Hare, F. Kenneth, Commissaire, Ontario Nuclear Safety Review, "The Safety of Ontario Nuclear Power Reactors". (1988)

(2) Comité consultatif de la sûreté nucléaire, "Recommandations et commentaires relatifs au Rapport sur la sûreté des centrales nucléaires de l'Ontario", rapport CCSN-15. (1988)

(3) Mosey, David et Weaver, Keith, "A Discussion of Institutional Failure and its Importance to Nuclear Safety", mémoire présenté à l'assemblée annuelle de 1988 de la Société nucléaire canadienne, Toronto. (1988)

(4) Penney, W., Schonland, B.F.J. Kay, J.M. et Diamond, J., "Report to the Chairman, UKAEA, on the Accident to the Windscale No. 1 Pile on October 10, 1957". (1957)

(5) Kemeny, John G., Président de la Commission présidentielle chargée de faire enquête sur l'accident à Three Mile Island, "The Need for Change: The Legacy of TMI". (1979)

(6) Brooks, G.L. et Siddall, E., "An Analysis of the Three Mile Island Accident", rapport EACL-7065. (1980)

(7) Commission de contrôle de l'énergie atomique, "Les répercussions de l'accident de Tchernobyl sur la sûreté des réacteurs CANDU", rapport INFO-0234. (1987)

(8) Howieson, J.Q. et Snell, V.G., "Tchernobyl - Le point de vue canadien", rapport AECL-9334. (1987)

(9) Ontario Hydro, "Submission to Ontario Nuclear Safety Review". (1987)

(10) Énergie atomique du Canada Limitée, "A Submission to the Ontario Nuclear Safety Review", rapport EACL-9427. (1987)

(11) Stevens, J.E.S. (EACL), lettre adressée à Margaret Grisdale (ONSR) en date du 13 juillet 1987, avec pièces jointes multiples. (1987)

(12) Association canadienne de normalisation, "Exigences relatives au programme d'assurance-qualité des centrales nucléaires", (CAN 3-Série N-286)

(13) Commission de contrôle de l'énergie nucléaire, "Programmes d'assurance-qualité des installations nucléaires", Document de consultation C-22. (1982)

(14) Comité consultatif de la sûreté nucléaire, "Exigences générales de sûreté recommandées pour les centrales nucléaires", rapport CCSN-4. (1983)

(15) Agence internationale de l'énergie atomique, "Basic Safety Principles for Nuclear Power Plants", rapport n° 75-INSAG-3 de la Collection sécurité de l'AIEA. (1989)

(16) Comité consultatif de la sûreté nucléaire, "Évaluation du rapport 75-INSAG-3 de la Collection sécurité de l'AIEA "Basic Safety Principles for Nuclear Power Plants"", rapport CCSN-16. (1989)

(17) Shemilt, L.W., Président, Comité technique consultatif sur le Programme de gestion des déchets de combustible nucléaire, "Dixième rapport annuel". (1989)

(18) Maxwell, R.B., communication privée. (1989)

ANNEXES

Nota : Sauf pour la rubrique intitulée "Defaillances institutionnelles", les attributions de défaillance hautement simplifiées, données entre parenthèses après chaque énoncé, représentent l'interprétation que le CCSN a faite de ce qui est indiqué dans les ouvrages de référence. Les notes figurant sous la rubrique "Défaillances institutionnelles" constituent des jugements portés par le CCSN à l'égard de ces défaillances.

L'attribution indiquée fait référence non pas à la personne, mais à l'institution responsable; à titre d'exemple, l'indication "erreur d'exploitation" signifie que la faute incombe à l'institution responsable de l'exploitation et de l'entretien.

L'indication d'un point d'interrogation (?) signifie qu'il est impossible de déterminer l'attribution en raison du manque d'information dans le document de référence.

Annexe 1 : États-Unis (Three Mile Island)

Sources : Références (5) et (6)

Séquence d'événements initiateurs :

- Blocage de la résine dans le filtre de polissage de l'eau d'alimentation (erreur de conception)
- Présence d'eau dans le système d'aération (erreur d'exploitation)
- Non-fermeture de la soupape de détente à commande par pilote (erreur de fabrication)

Causes premières :

- Ambiguité des témoins lumineux (erreur de conception)
- Non-respect des autres indications faisant état d'une perte de fluide de refroidissement (erreur d'exploitation)
- Réduction de l'injection d'eau à haute pression (erreur d'exploitation)

Causes aggravantes :

- Aucune mesure prévue en cas de formation d'hydrogène (erreur de conception)
- Mauvaise utilisation des filtres à l'iode (erreur d'exploitation)
- Non-étanchéité des systèmes de confinement (erreur de conception)

Causes concourantes :

- Défectuosité des filtres de polissage du condensat (erreur d'exploitation)
- Fermeture des vannes de coupure de l'eau d'alimentation de secours, indicateur non visible (erreur d'exploitation)
- Confusion dans les signaux transmis par les commandes, les alarmes et les indicateurs (erreur de conception)
- Procédures inadéquates (erreur d'exploitation)
- Mauvaise identification des conduits et des soupapes (erreur d'exploitation)

Causes sous-jacentes :

- Préoccupation à l'égard des règlements et du pire cas d'accident (erreur de réglementation)

- Formation déficiente des opérateurs (erreur de réglementation/d'exploitation)

- Procédures confuses, mauvaises pratiques (erreur d'exploitation)

- Mauvais entretien (erreur d'exploitation)

- Faiblesse de l'exploitant en sciences et en génie; lacunes au niveau de la gestion, des modes de fonctionnement de la centrale, de leur application et de leur surveillance, de l'assurance-qualité, de la vérification et de l'information fournie aux médias (faiblesse d'exploitation)

- Absence de plan d'urgence hors du site (lacunes en matière de protection civile)

- Lacunes au niveau de la réglementation, notamment quant à la structure, la gestion, le manque d'expérience exploitante et les failles sur le plan des inspections et de la surveillance de l'assurance-qualité et du contrôle de la qualité; problèmes non résolus et améliorations non abordées; aucune évaluation systématique de l'expérience; processus de certification ne tenant pas compte des défaillances doubles (lacunes au niveau de la réglementation)

Conclusions : La principale conclusion qui se dégage du rapport de la Commission Kemeny est que les problèmes fondamentaux concernent le personnel et non l'équipement. Il s'impose de modifier les organisations, les modes de fonctionnement et les pratiques, mais surtout les attitudes. Bien que de nombreuses conclusions précises jettent le blâme sur l'exploitant, un nombre aussi grand met en cause l'organisme de réglementation.

Défaillances institutionnelles

- Poursuite des activités en dépit de la non-étanchéité de la soupape de détente à commande par pilote (gestion chez l'exploitant)

- Absence de directive pour assurer que l'expérience d'un incident analogue, maîtrisé en sécurité à une autre centrale, soit communiquée aux autres exploitants de réacteurs similaires (organisme de réglementation)

- Lacunes dans les procédures d'exploitation qui ne tenaient pas compte des effets de deux phases dans le coeur sur les indications de niveau dans le pressuriseur (concepteur, gestion chez l'exploitant)

- Lacunes dans les procédures permettant la poursuite des opérations en dépit de la fermeture des vannes de coupure de l'eau d'alimentation auxiliaire (gestion chez l'exploitant)

- Procédures inadéquates en cas d'accident et responsabilités mal définies (gestion chez l'exploitant, organisme de réglementation)

- Plan d'urgence hors du site inadéquat (gestion chez l'exploitant, organisme de réglementation, autorités de l'État)

- Lacunes réglementaires, tel que décrit à la rubrique "Causes sous-jacentes" (organisme de réglementation)

- Lacunes de la part de l'exploitant, tel que décrit à la rubrique "Causes sous-jacentes" (gestion chez l'exploitant)

Annexe 2 : Union soviétique (Tchernobyl)

Sources : Références (7) et (8)

Événement initiateur :

- Tests effectués sans examen adéquat (erreur d'exploitation)

Causes premières :

- Exploitation du réacteur sans prévoir une marge de réactivité adéquate, ce qui est contraire aux règlements; exploitation du réacteur avec presque toutes les barres de commande retirées, ce qui constitue une infraction à la politique d'exploitation (erreur d'exploitation)
- Débit du liquide de refroidissement supérieur aux limites approuvées (erreur d'exploitation)
- Blocage des signaux de protection d'urgence, ce qui constitue une infraction à la politique d'exploitation (erreur d'exploitation)
- N'a pas respecté les imprimés d'ordinateur qui exigeaient l'arrêt immédiat (erreur d'exploitation)
- Blocage de l'arrêt d'urgence du réacteur sur turbo-alternateurs (erreur d'exploitation)

Causes aggravantes :

- Conception ne pouvant pas accommoder la défaillance d'un grand nombre de tubes de force (lacunes de conception/erreur de réglementation)
- Sections au-dessus de l'enceinte du réacteur à l'extérieur de l'enceinte de confinement (erreur de conception/ réglementation)
- Après exposition, le graphite très chaud a pris feu; il s'agit de la principale cause des décès et de la libération de substances radioactives (vulnérabilité de conception)
- Coeur enveloppé sans fluide de refroidissement pour éteindre l'incendie, ce qui a été une des principales causes de la libération de matières radioactives (lacunes au niveau de la protection civile)

Causes concourantes

- Remise à plus tard d'un test de mise en service (erreur de réglementation)
- Mauvaise préparation des protocoles d'essai (erreur d'exploitation)

- Pressions exercées sur les opérateurs afin de maintenir la production (erreur d'exploitation)

- Non-réglage du point de repère (erreur d'exploitation)

- Système d'arrêt du réacteur relativement lent, non indépendant du système de commande, non pleinement efficace dans toutes les conditions d'exploitation et pouvant en fait accroître la réactivité lors d'un arrêt d'urgence dans les conditions existant au moment de l'accident (vulnérabilité de conception)

Causes sous-jacentes

- Les principes de conception du réacteur reposaient en grande partie sur l'adoption de mesures appropriées de la part de l'opérateur (vulnérabilité de conception/erreur de réglementation)

- Conception du réacteur vulnérable aux accidents (vulnérabilité de conception/erreur de réglementation)

- Examen et surveillance inadéquats des opérations non courantes (erreur d'exploitation/de réglementation)

- Absence de plans d'urgence en cas d'accidents imprévus (lacunes en matière de protection civile)

Commentaire : Nos sources, qui proviennent des autorités soviétiques, jettent le blâme principalement sur les opérateurs. Il semble toutefois que l'organisme de réglementation doive assumer une partie de ce blâme, tout au moins à cause du manque de surveillance exercé. On pourrait même tenter de démontrer que l'accident de Tchernobyl est essentiellement imputable aux défaillances de l'organisme de réglementation.

Défaillances institutionnelles

- Exigences inadéquates concernant l'analyse de la sûreté des essais prévus (organisme de réglementation, gestion chez l'exploitant)

- Défaut d'inculquer aux opérateurs le souci de la sûreté (gestion chez l'exploitant, organisme de réglementation)

- Conduites d'exploitation permettant à un groupe de l'extérieur de diriger et de surveiller un essai prévu sans aucun contrôle apparent de la part de la direction de la centrale (gestion chez l'exploitant, organisme de réglementation)

- Défaut de reconnaître la nécessité d'un système de confinement adéquat et d'un système d'arrêt pleinement efficace (concepteur, organisme de réglementation)

- Défaut de reconnaître le danger potentiel de la conception de l'absorbeur de sûreté (concepteur, gestion chez l'exploitant, organisme de réglementation)

- Maintien de l'exploitation du réacteur avant l'accident avant que ne soit terminé le test de sûreté requis (gestion chez l'exploitant, organisme de réglementation)

- Défaut de reconnaître l'importance de séparer les fonctions de commande des fonctions de sûreté (concepteur, organisme de réglementation)

- Plans d'urgence inadéquats (autorités gouvernementales, organisme de réglementation)

Annexe 3 : Réacteurs Candu (en général)

Source : Référence (11) [P.j. = pièces jointes à la lettre]

P.j. 13 : Dépressurisation du circuit de caloportage, Bruce, 1975

- Erreur humaine durant l'entretien (erreur d'exploitation), aggravée par l'oubli du groupe de mise en service de communiquer (erreur d'exploitation) et par l'arrêt sans raison provenant d'une pompe (défaut de fabrication ?)

P.j. 14 : Fissures des tubes de force, Pickering, 1974 et 1983, Bruce 1986

- Erreur humaine dans l'installation des joints roulés (erreur de fabrication), aggravée par une inspection inadéquate (lacune au niveau de l'assurance-qualité) et par le défaut de prévoir un mode de défaillance (erreur de conception)

- Erreur humaine dans l'installation des ressorts d'écartement (erreur de fabrication), aggravée par une inspection inadéquate (lacune au niveau de l'assurance-qualité) et par une sous-estimation de l'accumulation de deutérium (erreur de conception)

- Défauts de fabrication des tubes (erreur de fabrication), aggravés par une inspection inadéquate (lacune au niveau de l'assurance-qualité) et par l'adoption de mauvaises pratiques d'exploitation pour localiser les fuites (erreur d'exploitation)

P.J. 16 : Activation du système refroidisseur un temps d'arrêt, Embalse, 1983

- Procédure d'exploitation inadéquate du système refroidisseur en temps d'arrêt et lacunes mineures dans d'autres procédures d'exploitation (erreur d'exploitation); système déclenché par l'arrêt de l'alimentation d'eau pour des raisons non précisées (défaillance de l'équipement?)

P.j. 17 : Perte de contrôle de l'eau d'alimentation, Embalse, 1983

- Présence d'eau et de poussières dans le système d'aération (erreur d'exploitation), aggravée par une programmation erronée dans le contrôleur (erreurs au niveau de la conception et de l'assurance-qualité)

- Erreurs de calcul lors de la programmation (erreur de fonctionnement)

P.j. 18 : Fuite d'eau lourde, Wolsung, 1984

- Quatre défauts de construction (erreurs de fabrication) non décelés (erreur au niveau de l'assurance-qualité) et erreur humaine mineure lors de l'entretien (erreur d'exploitation)

P.j. 19 : Enquête de suivi sur l'incident précédent

- Omissions dans la conception détaillée (erreurs de conception et au niveau de l'assurance-qualité), et référence à des "contacts ouverts non détectés" (erreur d'exploitation)

P.j. 20 : Mauvaise indication du niveau du liquide dans le système de contrôle des zones, Bruce, 1984

- Équipement exploité au-delà des limites de conception (erreur d'exploitation) et absence d'une procédure pour détecter une défaillance (erreur d'exploitation) et une défectuosité possible de l'instrument (erreur de fabrication)

P.j. 21 : Actionnement du mécanisme d'aspersion, Gentilly, 1985

- Attribuable semble-t-il à une procédure incorrecte (erreur d'exploitation)

P.j. 22 : Coup de bélier dans le système de refroidissement de secours du coeur, Embalse, 1986

- Défaut de montage électrique (défaut de fabrication) non décelé (erreur au niveau de l'assurance-qualité), provoqué par une erreur humaine lors de l'entretien (erreur d'exploitation); quelques lacunes dans le respect des procédures établies (erreur d'exploitation)

Défaillances institutionnelles

- En ce qui concerne la rupture des tubes de force (P.j. 14), la principale lacune de la part des institutions tient au fait qu'elles n'ont pas su prévoir et empêcher le mouvement des ressorts d'écartement; il s'agit donc de lacunes au niveau des programmes d'assurance-qualité (concepteur, gestion chez l'exploitant, organisme de réglementation)

- Dans le cas des tubes de force qui ont fui sans se rompre à Pickering et à Bruce (P.j. 14), la principale lacune concerne le programme d'assurance-qualité applicable à la fabrication et à l'installation des tubes de force (gestion chez l'exploitant responsable de la construction)

- Les autres incidents sont pour la plupart imputables à des erreurs humaines individuelles et à des lacunes de programmes d'assurance-qualité qui ne constituent pas des défaillances institutionnelles au sens du présent rapport.

Remerciements

Membres du groupe de travail

J.A.L. Robertson, président

N.C. Lind

J.T. Rogers

N.L. Williams

Membres du Secrétariat

R.J. Atchison

P. Smith (dactylographie)

Tous les membres du Comité consultatif de la sûreté nucléaire